TECHNOLOGY TRACK

TT460, Wireless Technology (WT)

Who Should Attend
DCIO/Federal Computer Crime Investigators.

Prerequisites
TT110 (INCH) or Test Out

Duration
5 Days

Course Description
Students examine wireless technologies from both a technical, and investigative perspective. Students learn basic wireless communication concepts that help them understand the capabilities and limitations of various wireless technologies. Common wireless network configurations are also examined. A number of hands-on exercises reinforce lecture material while providing students with first-hand knowledge of wireless vulnerabilities and monitoring techniques. {Mobile}

Objectives
- Recognize common wireless technologies
- Understand basic radio concepts
- Explain how Spread Spectrum Technology works
- Discuss common wireless network applications
- Define HomeRF, IrDA, Bluetooth, and Wi-Fi
- Recognize common wireless hardware components
- Identify how wireless devices communicate
- Build a wireless network
- Assemble a War Driving laptop or PDA
- Monitor a wireless network
- Discuss rogue wireless device detection methods
- Identify Jamming, WEP Key Cracking, Denial of Service, Session Hijacking, and Man-in-the-Middle attacks
- Harden a wireless network
- Summarize the DoD 8100.2 Directive

Topics Covered
Wireless Technologies
- Wireless Technologies Overview
- Basic Radio Concepts
- Spread Spectrum

Wireless Networks
- What is a Wireless Network?
- Types of Wireless Networks
- Hardware Components
- How Wireless Devices Communicate
- Building a Wireless Network

Wireless Vulnerabilities
- Wardriving
- Eavesdropping
- Accidental Association
- Rogue Access Points
- Attacks

TECHNOLOGY TRACK

Wireless Network Security

- Device Configuration
- Rogue Detection

What Every Investigator Needs to Know

- Identifying Wireless Devices
- Locating Wireless Network Devices
- Evidence
- Common Configurations

Preparation

To prepare for this course, we recommend the following review, reading, or research:

- Have a basic understanding of networking and the different types of wireless technologies, and topics, such as:
  - 802.11a, 802.11b, 802.11g, and 802.11n
  - Bluetooth
  - Infrared
  - WEP (Wired Equivalent Privacy)
  - WPA (WIFI Protected Access)
- Review printed material dealing with wireless technologies, and in CompTIA Network+ material. Additional information can be found in study guides for the Certified Wireless Network Administrator and Certified Wireless Security Professional certifications.

These topics are covered in DCITA courses you may have attended previously and can also be found on the dcita.edu portal (https://www.dcita.edu), the internet, at Books 24/7, in your organization's technical library or at the public library.

WT Grading Policy

Student progress is monitored through the use of instructor observation during lecture, discussion and practical exercises as well as a final Knowledge Test. Minimum passing score on all DCITA tests is 70%.